The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE

Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.

http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
10/11/2016

SUBJECT:
Multiple Vulnerabilities in Microsoft Graphics Component Could Allow for Remote Code Execution (MS16-120)

OVERVIEW:
Multiple vulnerabilities have been discovered in Microsoft Graphics Component, which could allow for remote code execution. These vulnerabilities can be exploited by either convincing a user to open a specially crafted document or visit a specially crafted webpage. Successful exploitation of these vulnerabilities could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

THREAT INTELLIGENCE:
There are reports of CVE-2016-3393 being exploited in the wild.

SYSTEMS AFFECTED:

- Microsoft Windows Vista, 7, 8.1, RT 8.1, 10
- Microsoft Windows Server 2008 and 2008 R2 (Including Server Core Installations)
- Microsoft Windows Server 2012 and 2012 R2 (including Server Core Installations)
- Microsoft Office 2007, 2010, and Word Viewer
- Skype for Business 2016, Microsoft Lync 2013, Microsoft Lync 2010, Live Meeting 2007
- Silverlight

RISK:
Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users: High

TECHNICAL SUMMARY:
Multiple vulnerabilities have been discovered in Microsoft Graphics Component, the worst of which could allow for remote code execution. The vulnerabilities are as follows:

- A remote code execution vulnerability exists in the way Windows Graphic Device Interface handles objects in memory (CVE–2016-3393).
- A remote code execution vulnerability exists in the way Windows Font Library improperly handles specially crafted embedded fonts (CVE-2016-3396).
- Multiple information disclosure vulnerabilities exist in the way that the Windows Graphics Device Interface handles objects in memory (CVE-2016-3209, CVE-2016-3262, CVE-2016-3263).
- An elevation of privilege vulnerability exists in the way that the Windows Graphics Component improperly handles objects in memory (CVE-2016-7182).
- An elevation of privilege vulnerability exists in the way that the Windows kernel fails to properly handle objects in memory (CVE-2016-3270).

Successful exploitation of these vulnerabilities could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

RECOMMENDATIONS:
The following actions should be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.
- Apply the Principle of Least Privilege to all systems and services.

REFERENCES:

Microsoft:
https://technet.microsoft.com/en-us/library/security/ms16-120.aspx

CVE:
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3209
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3262
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3263
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3270
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3393
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3396
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7182

TLP: WHITE

Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.

http://www.us-cert.gov/tlp/